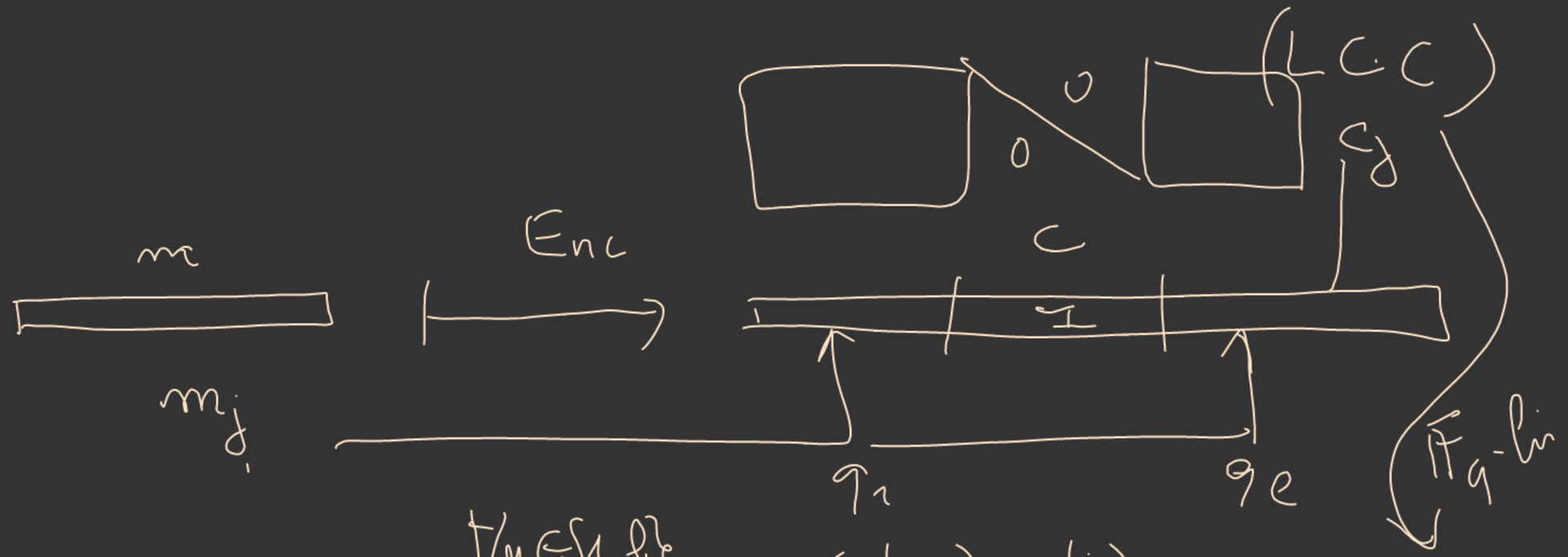


Alain LRC

I Guruswami-Sudan

II WTF? Bornes

III Folded Reed-Solomon

$\mathbb{F}_q$, $x_1 \dots x_n \in \mathbb{F}_q$ $\quad x_i \neq x_j$ $(i \neq j)$

$C = \left(f(x_1), \dots, f(x_n)\right)$; $\deg f < k \} = C_k$
$f \in \mathbb{F}_q[X]$

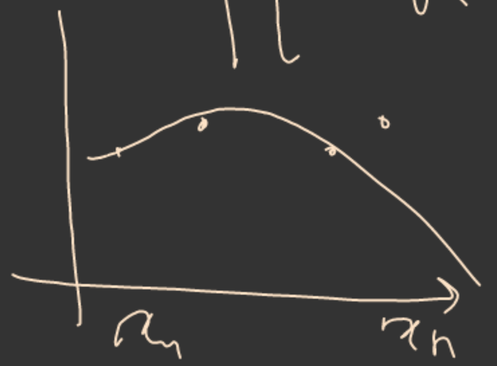
$y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$ "mot reçu" $\quad k \leq n$

$d(y, C_k) \leq \tau$

Pb: trouver $c \in C_k$ tq $d(y,c) \leq \tau$

$\Leftrightarrow$ $f \in \mathbb{F}_q[X]_{<k}$ tel que

$\left| \{ i, f(x_i) = y_i \} \right| \geq n - \tau$



Sudan - Guruswami (s auxiliaire)

① Trouver $Q(X,Y) \in \mathbb{F}_q[X,Y]$ t.q.

i) $Q(x_i, y_i) = 0$ (avec mult s)

ii) $\text{wdeg}_{1,k-1} Q(X,Y) < s(n-z)$

② Factoriser $Q(X,Y)$, trouver les facteurs $(Y - f(X))$

avec $\deg f(X) < k$, $d(c_q, y) \leq \tau$

Proposition $\forall f \in \mathbb{F}_q[X]_k$, $d(c_f, y) < z$, $\underline{Q(X, f(X)) = 0}$

- $\text{wdeg}_{1,k-1} Q(X,Y) < (n-z)s$ $\quad \deg Q(X, f(X)) < (n-z)s$
- $|\{ i,\ f(a_i) = y_i \}| \geq n - z$ $\quad \forall i \in \{1, n\}\ Q(a_i, y_i) = 0$

$|\{ i,\ Q(a_i, f(a_i)) = 0 \}| \geq n - z$

$Q(X, f(X))$ a plus de zéros que son degré $\Rightarrow Q(X, f(X)) = 0$

$Y - f(X) \mid Q(X,Y)$

Pourquoi $f(a_i) = y_i$ $\quad (X - a_i) \mid Q(X, f(X))$

$\geq s(n-z)$ $\quad \deg < s(n-z)$

Analyse du rayon r ?

$Q(X,Y) \neq 0$?

- $Q(x_i, y_i) = 0 \quad i \in \{1, n\}$
- $Q(X,Y) = \sum_{i=0}^{\ell} Q_i(X) Y^i$

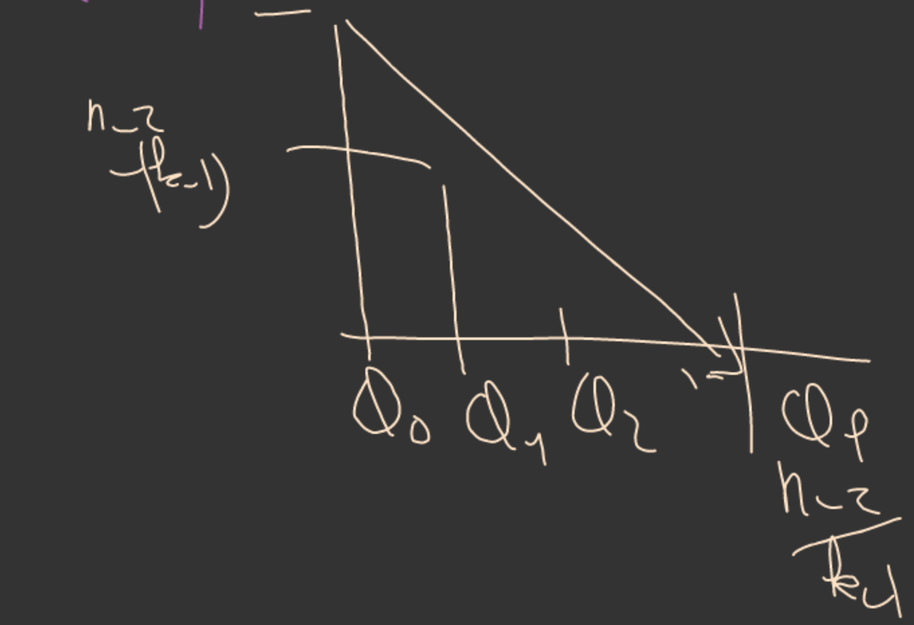
$N_Q > N_{eq} = n\binom{s+1}{2}$

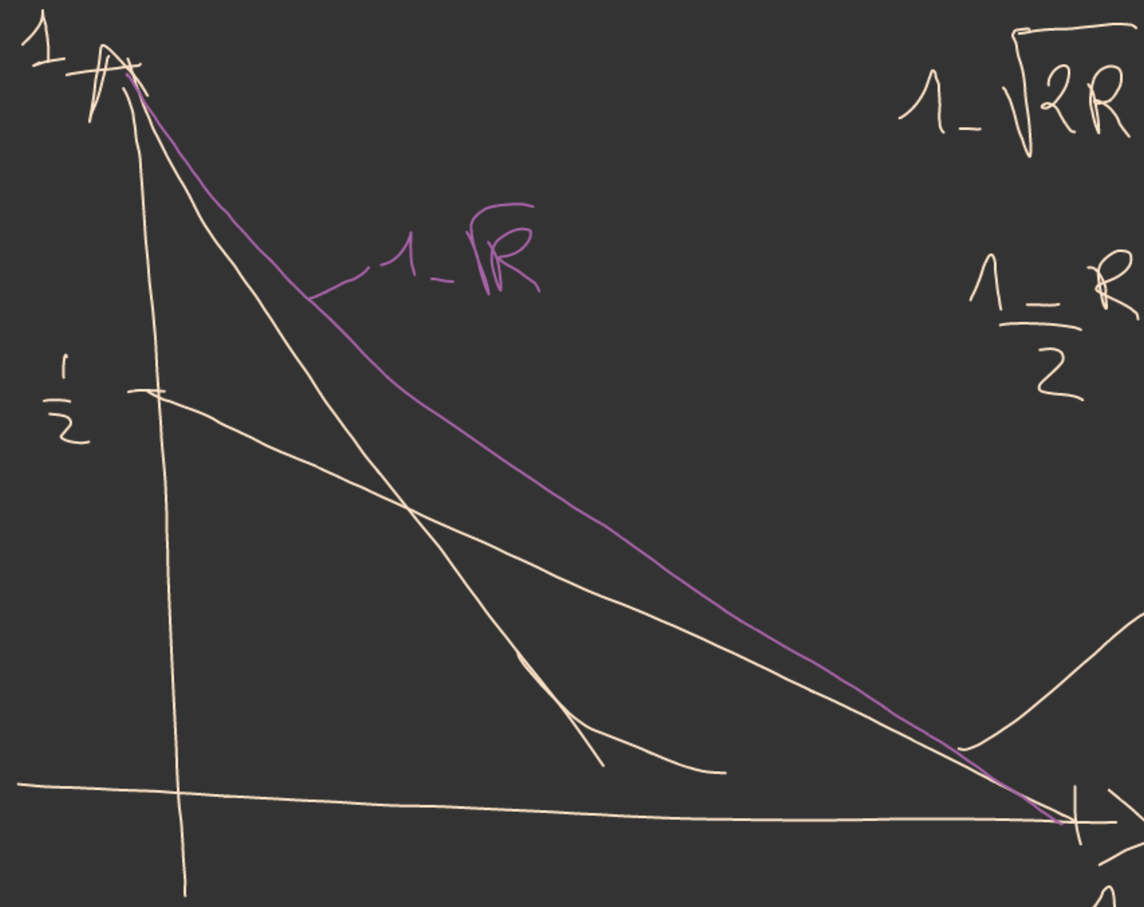
$\deg Q_i(X) \leq s(n-r) - (k-1)i$

$\frac{1}{2} s(n-r) \wedge \frac{n-r}{k-1} > n\binom{s+1}{2}$

$(n-r)^2 > 2n(k-1)$

$r < n - \sqrt{2n(k-1)\left(1+\frac{1}{s}\right)}$





$$1-\sqrt{2R} \simeq \frac{m-\sqrt{2(k-1)m}}{m}$$

$$\frac{1}{2}R = \frac{m-k}{2}\Big/ m$$

$$\frac{\tau}{n} = 1-\sqrt{R}$$

II Bornes

Déf Un code C est (ρ, ℓ)-décodable si $\forall y \in \mathbb{F}_q^n$

$$\left| B(y, \lfloor \rho n \rfloor) \cap C \right| \leq \ell$$

$\ell = 1 \rightsquigarrow t = \lfloor \frac{d-1}{2} \rfloor$

Théorème q fixé $\ell \geq 2$ $\rho \in [0, 1 - \frac{1}{q}]$ $(z = \lfloor \rho n \rfloor)$. $\exists$ ℓ existe une famille de codes (ρ, ℓ) asymptotique telle que

$$R \geqslant 1 - H_q(\rho) - 1/\ell$$

$R \gtrsim 1 - H_q(\delta)$

$\delta \simeq d/n$

$$R \geq 1 - H_q(p) - \frac{1}{e}$$

$$H_q(p) = p \log_q(q-1) - (1-p)\log_q(1-p) - p \log_q(p)$$

$p \log_q(q-1) \to p$

$(1-p)\log_q(1-p) \to 0$

$p \log_q(p) \to 0$

$\forall \varepsilon \exists C, q_{grand} \quad \underline{R = 1 - p - \varepsilon}$

$k = n \cdot d + 1$

$k/n = 1 \cdot d/n$

$R = 1 - \delta$

III Guruswami-Rudra

$x_1 \dots x_n \in \mathbb{F}_q$ $\quad C \subset \left((\mathbb{F}_q)^2\right)^n$ $\quad \mathbb{F}_q$-linéaire

$$\left\{ C = \left(\left(f(x_1), g(x_1)\right), \dots, \left(f(x_n), g(x_n)\right) \right) \;;\; \begin{array}{l} \deg f(X) < k \\ \deg g(X) < k \end{array} \right\}$$

$$y_j = \left(\left(y_{i,1}, y_{i,2} \right) \right)_{i=1 \dots n}$$

$$\left\{ (f,g) \;;\; \left| \left\{ i \;;\; f(x_i) = y_{i,1},\ g(x_i) = y_{i,2} \right\} \right| \geq n - \tau \right\}$$

$\deg f, \deg g < k$

① trouver $Q(X,Y,Z)$ tel que

- $\text{wdeg}_{1,k-1,k-1} Q(X,Y,Z) < s(n-z)$
- $Q(x_i, y_{i,1}, y_{i,2}) = 0$ (avec mult s)

② $Q(x, f(x), g(x)) = 0$

Analyse de z $\quad N_a > N_{eq}$

$$s(n-z) \times \frac{(n-z)^2 s^2}{6(k-1)^2} > n\binom{s+2}{3} \cdot 2$$

$$(n-z)^3 > ? \; n(k-1)^2 \left(1+\frac{1}{s}\right)\left(1+\frac{2}{s}\right)$$

$$z < n - \sqrt[3]{2n(k-1)^2 \left(1+\frac{1}{s}\right)\left(1+\frac{2}{s}\right)}$$

$$R = 2k/n$$

$$\frac{z}{n} < 1 - R^{2/3} \qquad (1-\sqrt{R})$$

$$\left(\frac{z}{n} < 1 - R^{m/m+1}\right) \qquad \uparrow \text{GS}$$

$$\varphi(x, y, z)$$

$$\varphi(x, f(x), g(x)) = 0$$

$$y = f(x) \qquad z = g(x)$$

Folded RS

n pair $\quad x_0 \dots x_{n-1} \in \mathbb{F}_q \quad$ 2-replié

$$c = \left(f(x_0) \dots f(x_{n-1}) \right) \qquad \deg f < k$$

$$c_2 = \left(\begin{bmatrix} f(x_0) \\ f(x_1) \end{bmatrix} \; f(x_2) \; f(x_3) \; \dots \; \begin{bmatrix} f(x_{n-2}) \\ f(x_{n-1}) \end{bmatrix} \right) \in \left(\mathbb{F}_q^2 \right)^{n/2}$$

$\langle \gamma \rangle = \mathbb{F}_q^*$

$x_i = \gamma^i$

$f(X) \to f(\alpha X)$

$$y = \left((y_{i,1}, y_{i,2}) \right)_{i=0 \dots \frac{n}{2}-1}$$

① $Q(\gamma^i, y_{i,1}, y_{i,2}) = 0$ (avec mult s)

② $\text{wdeg}_{1,k-1,l-1} Q(X,Y,Z) < s(n-2)$

$$\left| \{ i \text{ pair} \mid f(x_i) = y_{i,1} \;\; f(x_{i+1}) = y_{i,2} \;\; f(\gamma x_i) = y_{i,2} \} \right|$$

$$Q(x_i, f(x_i), f(\gamma x_i)) = 0 \quad (\text{mult } s)$$

$$Q(X, f(X), f(\gamma X)) = 0$$

trouver les $f(x)$, $\deg f(x) < k$ telque $Q(x, f(x), f(\gamma x)) = 0$

Prop $X^{q-1} - \gamma$ est irréductible sur $\mathbb{F}_q$

$$f(x)^q = f(x^q)$$
$$= f(\gamma x) \mod (X^{q-1} - \gamma)$$
$$Q(x, \gamma, \gamma^q) = 0 \mod (X^{q-1} - \gamma)$$
$$H(Y) \in \mathbb{F}_{q^r}[Y]$$

m - reflié

$$Q(x, f(x), f(\gamma x) \ldots f(\gamma^{m-1} x)) = 0 \; ?$$

$$Q(x, f(x), f(x^q), \ldots f(x^{q^{m-1}})) = 0 \qquad (x^{q-1} - \gamma)$$

$$\#(Y) = 0$$